STATE OF DELAWARE

OFFICE OF AUDITOR OF ACCOUNTS

DEPARTMENT OF EDUCATION

GENERAL INFORMATION SYSTEM CONTROLS FOR THE ESCHOOLPLUS PROCESSING ENVIRONMENT

FEBRUARY 19, 2004 - MARCH 31, 2004

INFORMATION SYSTEMS AUDIT

R. THOMAS WAGNER, JR., CGFM, CFE
AUDITOR OF ACCOUNTS

EXECUTIVE SUMMARY

BACKGROUND

The Department of Education (Department), located in Dover, serves 19 school districts and 13 charter schools. Technology issues within Department are primarily the responsibility of the Technology Management & Design Group. This group, within the Assessment & Accountability Branch, is tasked with five primary areas of responsibility: statewide student and staff data collection, data analysis and reporting, design and development of information systems, operation of the Department Computer Center and communications network, and management of statewide software licenses.

The Delaware Student Information System (DELSIS) is the master student database used by Department for creation of student identification numbers, for tracking students through Delaware schools, and for generating reports based on current and historical student data. The eSchoolPlus system interfaces with DELSIS to provide both summary and detail level information from the actual school/district to Department which is necessary to meet the many reporting requirements necessary in the area of student accounting.

As of January 2004, eSchoolPlus is in place and being used at the following school districts: Cape Henlopen, Woodbridge, Campus Community, Delaware Military Academy, and Providence Creek Academy for managing student data. The Department is in the process of training the following four schools to migrate to the eSchoolPlus system: Brandywine, Colonial, Red Clay, and Christina. The Department's intention is to migrate all schools to eSchoolPlus by January 2005.

AUDIT OBSERVATIONS AND CONCLUSIONS

Notwithstanding the progress made thus far, significant efforts are needed to improve the general controls over the integrity, confidentiality, and availability of information and systems at the Department of Education Computer Center (DOECC). General controls weaknesses were noted in various areas, posing risk of unauthorized access, modification, and destruction of information resources at the Computer Center. Several of the general controls weaknesses identified can greatly impact the effectiveness of the department's ability to carry out responsibilities and activities as intended. Without effective Information Technology controls, Department management cannot be reasonably assured that information resources are protected from intentional or unintentional errors and unauthorized use.

We found controls weaknesses in the following areas relative to the eSchoolPlus general information system controls processing environment:

- Application Software Development - The Department has not established written policies and procedures for control of changes to the eSchoolPlus pupil accounting

system. Furthermore, the department does not document or maintain system change requests for modifications to the system.

- Service Continuity - We found the Department does not have a comprehensive disaster recovery plan for the computer center. Furthermore, the DOECC has not established written policies and procedures for server backup and recovery that incorporate the eSchoolPlus application and underlying database servers.

- Manage Problems and Incidents - According to the Department IT personnel, formalized procedures for the help desk function have not been developed. The Department has recognized the need for a help desk function and has purchased software to create consistency among help desk personnel.

- Access to Computer Resources

  - Logical Access to Computer Resources - The Department has not established written policies and procedures for granting and revoking logical access to the eSchoolPlus pupil accounting system. When a user's ID is established, there are no formal standards for the system administrator to follow in establishing access. Furthermore, a user working for a school district was granted direct access to databases stored on the database server supporting the eSchoolPlus application. At the time of our review, the user had been given read, write, insert, and update access to two production databases stored on the database server.
  - Physical Access to Computer Resources - We identified 14 employees and 3 contractors whose job duties and responsibilities did not require them to have physical access. Physical security of the Department's wiring racks in the Townsend Building were found to be unsecured. A lack of appropriate physical security inside the computer center was also identified. Potential problems included: a wooden door separating an office from the data center, no closer on the south-end computer center door, entry to the data center is accessible through an adjoining agency's office space, and lack of an entry log for visitors. Additionally, the Uninterruptible Power Supply (UPS) used to supply immediate backup power for all equipment located in the computer room is in an unsecured area.
  - Manage Software and Hardware - The Department does not maintain complete and accurate inventory records of IT physical assets or software. The Department has not developed formal policies and procedures to identify and ensure accountability of software and the Department needs to documented policies and procedures to clear sensitive information and software from computers, disks, and other media prior to disposal.

- System Software Controls

  - Maintenance and Monitoring - Event logs for those servers supporting the eSchoolPlus application indicated numerous error events that required follow-up and correction. However, we found no evidence that the error events were

periodically reviewed and corrected. The Department utilizes an automated patch management tool for maintaining patches on Departmental computers and servers. However, we found the web server hosting the eSchoolPlus application was missing two critical operating system patches. In addition, the Department has not developed formal policies and procedures to address patch management.

- Operating System Installation Parameters - The Department has not taken the necessary measures to reduce the risk of unauthorized access to the Web server hosting the eSchoolPlus application or the database server supporting the eSchoolPlus application. Our evaluation identified system configurations that are vulnerable to unauthorized access due to the fact that the Department did not make the appropriate modifications to the operating system's default configuration to adequately safeguard the database and web servers from potential vulnerabilities.
- Software Licenses - We were informed that the database software supporting the eSchoolPlus application has not been properly licensed. The auditors brought this to the attention of the Department management.

AGENCY RESPONSE

The Delaware Department of Education has agreed with the findings and recommendations as presented in this audit report and has prepared an acceptable plan of corrective action. The Department's detailed response has been included with the findings and recommendations within this report.

TABLE OF CONTENTS

AUDIT AUTHORITY

Title 29, Del. C. c. 29 authorizes the Auditor of Accounts to perform postaudits of all the financial transactions of all State agencies. The law requires that the audits be made in conformity with generally accepted auditing principles and practices. Such principles and practices are established by two standard setting bodies: the American Institute of Certified Public Accountants, which has issued generally accepted auditing standards; and the U.S. General Accounting Office, which has issued generally accepted government auditing standards.

Auditing standards issued by these organizations require the auditor to obtain an understanding and evaluate an entity's internal controls related to computer systems that process information used in preparing an entity's financial statements and administering governmental programs. Furthermore, governmental auditing standards require auditors to obtain sufficient, competent, and relevant evidence that computer processed data are valid and reliable. Auditors may view the computer system control activities in terms of general and application controls.

General controls are policies and procedures that relate to many applications and support the effective functioning of application controls by helping to ensure the continued proper operation of information systems. General controls commonly include controls over data center and network operations; system software acquisition and maintenance; access security; application system acquisition, development and maintenance and service continuity.

Application controls apply to the processing of individual applications. These controls help to ensure that transactions occurred, are authorized, and completely and accurately recorded and processed. Examples include edit checks of input data, numerical sequence checks, and manual follow-up of exception reports.

BACKGROUND

In Delaware, the Department of Education (Department), located in Dover, serves 19 school districts and 13 charter schools. The mission of Department is to promote the highest quality education for every Delaware student by providing visionary leadership and superior service. Department is headed by a cabinet Secretary and consists of approximately 192 staff members. The Department's major funding source was the State General Fund. The General Fund expenditures for Fiscal Year 2003 were approximately $794 million and the recommended budget, including appropriated special funds, for Fiscal Year 2004 is $814 million.

The Department is comprised of three distinct branches: Curriculum and Instructional Improvement; Assessment and Accountability; and Finance and Administrative Services. Technology issues within the Department are primarily the responsibility of the Technology Management & Design Group. This group, within the Assessment & Accountability Branch, is tasked with five primary areas of responsibility: statewide student and staff data collection, data analysis and reporting, design and development of information systems, operation of the Department of Education Computer Center (DOECC) and communications network, and management of statewide software licenses. Currently the DOECC staff has the responsibility of supporting and maintaining 72 servers and 244 desktop computers. These servers and computers are located at 4 different locations: the Townsend Building in Dover; the William Penn Building in Dover; the Science Resource Center in Smyrna; and the Higher Education Commission in Wilmington.

The Department is responsible for providing centralized statewide data management for public education. The data management activities include the Delaware Student Information System (DELSIS). DELSIS is the master student database used by the Department for creation of student identification numbers, for tracking students through Delaware schools, and for generating reports based on current and historical student data. Currently many schools must either crosswalk their pupil accounting system IDs to DELSIS, or must manually enter data in both systems. DELSIS has six interfaces: FACTS, SASSI, spreadsheets from the charter schools, Pentamation, eSchoolPlus, and the data service center. Pentamation is a client-server application running at the Department Computer Center and is being used by many of the state's 19 school districts. Eleven school districts and several charter schools are currently using the open series of Pentamation. However, Pentamation is in the process of being upgraded to a web-based version called Web SMS (eSchoolPlus). As of January 2004, eSchoolPlus has been in production and is implemented in the following school districts: Cape Henlopen, Woodbridge, Campus Community, Delaware Military Academy, and Providence Creek Academy for managing student data.

As the client-server version of Pentamation is at the end of its life cycle, the Department's plan is to migrate the student accounting function to a web-based application. Currently, the Department is in the process of training the following four schools to migrate to this new application: Brandywine, Colonial, Red Clay, and Christina. The intention is to migrate all the schools to eSchoolPlus by January 2005. The general controls consist of determining whether

the structure, policies, and procedures of the data management activities help to ensure the proper operation, data integrity, and security of those systems maintained by the DOECC. The application controls consist of determining whether the structure, policies, and procedures provide reasonable assurance that data entered into eSchoolPlus is valid, properly authorized, and completely and accurately processed.

OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

The objective of the audit was to determine whether the structure, policies, and procedures help to ensure the proper operation, data integrity, and security of those systems maintained by the Department of Education Computer Center (DOECC). To determine this overall objective, we conducted our audit to:

- Determine the adequacy and effectiveness of controls over hardware purchases and disposal.
- Determine if appropriate physical security and access to facilities provide suitable controls that protect the IT equipment and people against man-made and natural hazards.
- Determine if appropriate environmental controls have been established to protect the IT equipment and people against man-made and natural hazards.
- Determine if adequate logical security controls have been established to protect the integrity and confidentiality of sensitive files.
- Determine if the Department has implemented adequate controls over IT operations to ensure that data remains complete, accurate, and valid during its input, update, and storage.
- Determine the adequacy of the Department's preparedness to address and effectively react to emergency situations.
- Determine the adequacy of hardware preventative maintenance practices.
- Evaluate the strategy, policies, standards, procedures, and related practices for the management and planning of Information Technology.
- Determine the level of training and proficiency of those IT personnel supporting the eSchoolPlus application.
- Determine whether end users are properly trained to effectively and efficiently utilize the eSchoolPlus application.
- Evaluate the adequacy and security of documentation maintained for general and specific computer operations and applications.
- Evaluate the stability of the vendor of the eSchoolPlus application.
- Determine the satisfaction of end users of the eSchoolPlus application.
- Determine whether the database server supporting the eSchoolPlus application has been securely configured.
- Determine whether the web server supporting the eSchoolPlus application has been securely configured.

SCOPE

We reviewed the general controls surrounding the eSchoolPlus application at the Department. Our planned audit scope included a review of the eSchoolPlus application controls, but because of the significant general control weaknesses identified and as application controls are dependent upon effective general controls, an audit of the eSchoolPlus application controls was not conducted. Our fieldwork was performed at the DOECC center located in the Townsend Building, Dover, Delaware. We conducted our fieldwork from February 19, 2004 through March 31, 2004.

METHODOLOGY

We conducted this audit in accordance with generally accepted government auditing standards. Our procedures consisted of interviews with Department, school district, and charter school personnel, an end user satisfaction survey, reviewing policies and procedures in place at the Department, and performing tests of key control features to confirm our understanding and the effectiveness of these controls. We reviewed the control policies and procedures for the following areas:

- Inventory Controls
- Physical Security
- Environment Controls
- Logical Security
- Data Integrity
- Service Continuity
- Equipment Maintenance
- Management
- Training
- Documentation
- Vendor Relations
- Operations
- SQL Server 2000
- Internet Information Services (IIS)

The criteria used in the performance of this audit consisted of *Internal Control-Integrated Framework*, published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO); *CobiT: Control Objectives for Information and related Technology*, published by the Information Systems Audit and Control Foundation; and the State of Delaware *Budget and Accounting Policy Manual.*

FINDINGS AND RECOMMENDATIONS

EX.1: Physical Access Controls (Electronic)

Finding:
We reviewed the 22 employees/contracted personnel that had been issued access cards for the computer center. We identified 14 employees and 3 contractors whose job duties and responsibilities did not require them to have physical access. Physical access to the computer center is controlled by an electronic cardkey system. We further noted that there are no written policies and procedures regarding the issuance and/or revocation of these access cards. It is important to establish policies and procedures to control entry into the computer center. Unauthorized physical access to any information systems area substantially increases the risk of physical damage, unauthorized disclosure of information, loss of control over system integrity, interruptions in providing computer services, or physical theft.

Recommendation:
We recommend the Department review the list of access card holders and remove those employees/personnel for which physical access to the computer center is not required for their normal job duties.

We further recommend policies and procedures be established for the issuance and revocation of computer center access cards. These policies and procedures should include (but not be limited to) a standard form requiring management authorization, periodic monitoring of the access logs, responsibilities of card holder, and periodic review of necessity for those assigned access cards to the computer center.

Management Response:
"Agree. An IT Audit implementation committee has been created. This committee has asked our new security staff member to identify those who should have access. This list will be reviewed by the entire committee and access will be denied to any unessential personnel. In addition the committee will begin work on the necessary procedures and policies as recommended."

Approximate Date of Expected Completion:
Access restrictions will be in place by April 21, 2004. Policies and procedures will be completed by June 30, 2004.

EX.2: Change Management

Finding:
The Department does not document or maintain system change requests for the eSchoolPlus pupil accounting system. Changes to an application should be clearly documented, tested, and authorized by management and the end-users. The use of standardized change request forms

help to ensure that requests are clearly communicated and that approvals are documented. Change request forms should be maintained for at least as long as a system is in operation in case questions arise regarding why or when system modifications were made.

The establishment of a change management policy for an organization is a vital step in controlling system maintenance work. A change management policy should describe in broad terms the responsibilities, authorities, functions, and operations of the change management function. It should be sufficiently comprehensive to address any type of change to the computer-based application system and its environment, including changes to the hardware, software, and firmware. To be effective, the policy should be consistently applied and must be supported and promulgated by upper management to the extent that an organizational commitment to change management is established.

Undocumented changes to systems results in a lack of adequate records of who made the change, when the change was made, and a description of the change made. In addition, if authorization procedures have not been developed or are not followed, an individual might be able to initiate program changes that result in erroneous processing and/or weakened access controls of the system.

Recommendation:
We recommend the Department establish and implement written policies and procedures for all system changes. These policies and procedures should address (at a minimum) formal documentation, authorization, testing, and approval.

Management Response:
"Agree. The IT committee is currently reviewing a change management system. This system will be demonstrated for TMD staff and recommendations will be made for purchase. A change Management process will then be developed and implemented."

Approximate Date of Expected Completion:
January 30, 2005.

EX.3: Monitoring

Finding:
We reviewed the event logs for those servers supporting the eSchoolPlus application and found numerous error events that required follow-up and correction. However, we found no evidence that the error events were periodically reviewed and corrected. Inquiry of IT personnel confirmed that the Department does not periodically review performance, system, security, and other event logs. In addition, the Department does not have policies and procedures for periodically reviewing event logs. A periodic review of system-generated logs can detect security problems, performance issues, and other irregularities including attempts to exceed authority or gain system access during unusual hours. Irregular events should be followed up on to determine the cause of the event and corrective action taken if deemed necessary.

Recommendation:
We recommend that management implement policies and procedures to ensure Information Technology personnel periodically review, document, and take prompt action on, irregularities identified in performance, system, security, and other computer event logs. In implementing this recommendation we encourage the Department to consider the use of automated software to assist the system administrators in the identification of critical events.

Management Response:
"Agree. TMD has purchased a series of products from Computer Associates. UniCenter is the product that we currently are in the beginning stages of implementation. This product will allow us to meet the monitoring finding."

The implementation of this recommendation will be handled through the software and not be implemented as the manual system outlined in the recommendation.

Approximate Date of Expected Completion:
Policies and procedures will be completed by June 30, 2004. Full implementation of the system will be completed by June 30, 2005.

EX.4: Internet Information Services (IIS)

Finding:
The Department has not taken the necessary measures to reduce the risk of unauthorized access to the Web server hosting the eSchoolPlus application. Our evaluation of the Windows® 2000 Internet Information Services (IIS) server hosting the eSchoolPlus application identified a system configuration that was vulnerable to unauthorized access. IIS security is tightly coupled to the operating system and, by default, Microsoft® Windows® 2000 installations contain numerous potential security problems including several unneeded services that are installed and enabled, minimal event logging, and no active local security policy. The Department did not make the appropriate modifications to the operating system's default configuration to adequately safeguard the web server and eSchoolPlus application from potential vulnerabilities.

Recommendation:
We recommend the Department develop and implement a standard system configuration based upon manufacturer's security hardening recommendations or "best practices" to significantly reduce the risk of unauthorized access to be used for all Microsoft® Windows® 2000 computers running Internet Information Services (IIS).

Management Response:
"Agree. The audit reviewed only eSchoolPlus servers as we move from beta to production the department will follow the same procedures for the eSchooPlus servers that we do for the rest of the DDOE environment. The servers in the DDOE environment would comply with this recommendation."

Approximate Date of Expected Completion:
August 31, 2004.

EX.5: Patch Management

Finding:
The Department utilizes an automated patch management tool for maintaining patches on Departmental computers and servers. However, at the time of our review the web server hosting the eSchoolPlus application was missing two critical operating system patches. In addition, the Department has not developed formal policies and procedures to address patch management. A patch is an interim fix usually developed and distributed by the software vendor as a temporary resolution to an identified problem with the software. The first line of defense in maintaining a secure operating system is up-to-date patches. Depending on the vulnerability, failure to apply patches could result in unauthorized disclosure of information, loss of control over system integrity, or interruptions in providing computer services. In addition, because exploits relating to announced vulnerabilities are materializing faster (Blaster appeared only 26 days after Microsoft reported the vulnerability) it is imperative that patches are applied in a timely manner.

Recommendation:
We recommend the Department periodically verify the servers supporting the eSchoolPlus application include all critical patches and service packs for the Operating System. We further recommend the Department develop written policies and procedures to address patch management.

Management Response:
"Agree. The IT audit committee agrees with the finding. We are in the process of upgrading our automatic patch system to PatchLink. This system will allow us to more closely monitor glitches in patch downloads. We are also in the process of developing written policies and procedures to address patch management."

Approximate Date of Expected Completion:
June 30, 2004.

EX.6: Wiring Closet

Finding:
Telecommunications resources were not physically secure. As part of our review of general controls, we conducted a physical survey of the Department's work space in the Townsend Building and discovered that the wiring racks were not physically secured, and in some instances were accessible to any visitor to the Townsend Building. Insecure wiring racks could allow damage to equipment, unauthorized monitoring, or disruptions in service via malicious or unintentional activities. Physical access controls should provide reasonable assurance that computer related facilities and equipment are protected against unauthorized access and use.

Recommendation:
We recommend the Department physically secure the wiring closets within the Townsend Building.

Management Response:
"Agree. This finding will be addressed by the Department at the Cabinet Level."

Approximate Date of Expected Completion:
Tentatively scheduled for December 31, 2004.

EX.7: Unlicensed Software

Finding:
In an interview with IT personnel we were informed that the database software supporting the eSchoolPlus application has not been properly licensed. The auditors brought this to the attention of Department of Education management during the update meeting held on March 16, 2004. The Department of Education's *Computer Policy* states, "It is the policy of the Department that **NO SOFTWARE** will be used which has not been purchased." The use of unauthorized copies of a software product may constitute copyright infringement, for which the Department may be subject to civil and/or criminal penalties. In addition, unlicensed copies of software may lack the quality controls built into the licensed versions, making the copies far more prone to computer viruses. Unlicensed software may also be an old version of the application with defects, incomplete files, or inadequate documentation; the data processed by such applications may not be reliable. Moreover, access to documentation, free technical support and upgrades are typically unavailable for unlicensed software.

Recommendation:
We recommend the Department obtain the proper software license for the database software supporting the eSchoolPlus application.

We further recommend management implement procedures to ensure all software is licensed in accordance with vendor requirements and the Department's *Computer Policy*.

Management Response:
"Agree. This finding has been addressed."

Approximate Date of Expected Completion:
Completed.

EX.8: Help Desk Policies and Procedures

Finding:
According to the Department IT personnel, formalized procedures for the help desk function have not been developed. The Department has recognized the need for a help desk function and

has purchased software to create consistency among help desk personnel. Without written policies and procedures the efficiency and effectiveness of help desk functions may be negatively impacted. While a training program acquaints a user with a software package and its basic operations, policies and procedures are needed as a long-term comprehensive reference guide to software use, features, and design. User procedures are generally the only guide to infrequently used operations and is also necessary as a diagnostic aid when the software does not work as expected.

Recommendation:
We recommend that the Department establish written policies and procedures for the help desk function. The help desk policies and procedures should include, but not be limited to:

- Develop written problem isolation and determination procedures.
- Develop written problem escalation procedures that prioritize the type of problems reported and establish call back times based on the urgency of the problem reported.
- Develop metrics to assess the timing, frequency, and source of problems to aid in the monitoring and performing trend analysis for early identification of systemic problems (i.e., running out of space on a server).
- Requirement that a problem ticket be prepared for all problems reported.

Management Response:
"Agree. The eSchoolPlus help desk is in the process of being implemented. The beta sites for this product worked directly with SunGuard Pentamation to report any problems."

Approximate Date of Expected Completion:
August 15, 2004.

EX.9: Hardware Inventory

Finding:
Our review of the inventory process revealed the Department does not maintain complete and accurate inventory records of IT physical assets. Management must ensure that adequate internal controls are in place to protect inventories of items for which there is an inherent risk of loss, theft, or misuse. When complete and accurate inventory records are not maintained and established control procedures are not followed, the Department cannot ensure proper safeguarding, reporting and accountability of state property and equipment.

Property inventory records should be maintained that include:

- a description of the property,
- a serial number or other identification number,
- the source of property,
- who holds title,
- the acquisition date,
- cost of the property,

- percentage of Federal participation in the cost of the property,
- the location, use and condition of the property, and
- any ultimate disposition data including the date of disposal and sale price of the property.

In addition, a physical inventory of the property should be taken and the results reconciled with the property records at least annually. Periodic inventories help identify assets that may have been misplaced or misappropriated.

Recommendation:
We recommend that the Department establish formal policies and procedures requiring the preparation and maintenance of inventory records to identify and ensure the accountability of assets. Inventory records should include at a minimum the description of the property, serial number, acquisition date, cost, source, location, condition of property, date of disposal, and sale price. Additionally, periodic physical inventory reconciliation of assets should be conducted at least annually.

Management Response:
"Agree. TMD will be working with Finance and Administrative Branch to develop Department policies as recommended."

Approximate Date of Expected Completion:
December 15, 2004.

EX.10: Logical Security Administration

Finding:
We found the Department has not established written policies and procedures for granting and revoking logical access to the eSchoolPlus pupil accounting system. When a user's ID is established, there are no formal standards for the system administrator to follow in establishing access. In addition, procedures are not in place to consistently ensure access is properly approved, which may allow employees and contractors to have unnecessary access to data. Also, access authorization documentation is not maintained for users.

Information resources security access controls provide reasonable assurance that data are protected against unauthorized use, modification, disclosure, loss, or impairment. Inadequate access controls diminish the reliability of computer processed data and increase the risk of destruction or inappropriate disclosure of information. The purpose of controlling access to data and information is to ensure (1) users have only the access needed to perform their duties, (2) access to sensitive resources is limited to only those for which it is required to carryout their job functions, and (3) employees are restricted from performing incompatible functions or functions beyond their responsibility.

Inadequate controls over the establishment of user and group profiles increases the risk of being unable to ensure that user access rights are commensurate with their job function and unauthorized access to system resources may occur.

Recommendation:
We recommend the Department establish and implement written policies and procedures for granting, revoking, modifying and monitoring access to data and information systems. These policies and procedures should include, but not be limited to:

- Required written authorization forms signed by the user and the data owner before access is granted;
- Performing and documenting periodic (i.e. annual) reviews of user access to determine sufficiency; and
- Standard naming conventions to be used for the assignment of user and/or system accounts.

Management Response:
"Agree. The Department will bring the eSchoolPlus project in line with other DDOE systems."

Approximate Date of Expected Completion:
August 15, 2004.

EX.11: Physical Security of Computer Center

Finding:
A lack of physical security inside the computer center was identified during a walkthrough of the server facility. Observations included a wooden door separating an office from the data center, no closer on the south-end computer center door, entry to the data center is accessible through an adjoining agency's office space, and lack of an entry log for visitors.

Appropriate physical security and access control measures should be established for IT facilities. Physical security and access controls should address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting services (such as electric power), backup media and any other elements required for the system's operation. Access should be restricted to individuals who have been authorized to gain such access. Where IT resources are located in public areas, they should be appropriately protected to prevent or deter loss or damage from theft or vandalism.

Physical security controls restrict physical access to computer resources and protect them from intentional or unintentional loss or impairment. By obtaining unrestricted access to computer resources, an individual could obtain access to terminals or telecommunications equipment causing intentional or unintentional loss or impairment.

Recommendation:
We recommend that the physical security of the computer center be enhanced to include the following:

- The wooden door inside the computer center be replaced with a heavier steel door.
- A closer be installed on the south-end computer center door.

- A lock be installed on the adjoining agency's door accessing the computer center.
- An entry log for visitors be maintained.

Management Response:
"Agree. Department will be working with Administrative Services to bring the computer center into compliance. Many of these are in the process of being corrected."

Approximate Date of Expected Completion:
This is dependent on work by Administrative Services.

EX.12: Disaster Recovery Plan

Finding:
We found the Department does not have a comprehensive disaster recovery plan for the DOECC. A comprehensive disaster recovery plan is necessary to protect information resources, minimize the risk of unplanned interruptions, and recover critical operations should interruptions occur. Losing the capability to process, retrieve, and protect information maintained electronically can significantly affect an agency's ability to accomplish its mission.

Recommendation:
We recommend that a disaster recovery plan be developed which will help to protect information resources, minimize the risk of unplanned interruptions, and help to ensure the timely recovery of critical operations should interruptions occur.

Management Response:
"Agree. In progress."

Approximate Date of Expected Completion:
June 30, 2004.

EX.13: Backup Policies and Procedures

Finding:
We found the DOECC has not established written policies and procedures for server backup and recovery that incorporate the eSchoolPlus application and underlying database servers. The Department routinely copies data files and software and securely stores these files at a remote location to mitigate service interruptions. Backup policies and procedures are necessary to ensure the efficient recovery of data and operations in the event of a computer operations disruption. The development of written policies and procedures will encourage stability and continuity in operations, circumvent ambiguity and confusion about procedures, and discourage actions based upon personal individuality.

Recommendation:
We recommend the Department establish written policies and procedures for backup and recovery to include the eSchoolPlus application and underlying database servers.

Management Response:
"Agree. In progress."

Approximate Date of Expected Completion:
June 30, 2004.

EX.14: Disposal Policy

Finding:
We found the Department does not have documented policies and procedures in place to clear sensitive information and software from computers, disks, and other media prior to disposal. Management should define and implement procedures to prevent access to sensitive information and software from computers, disks and other equipment or media when they are disposed of or transferred to another use. If sensitive information is not fully cleared, it may be recovered and inappropriately used or disclosed by individuals who have access to discarded equipment.

Recommendation:
We recommend that the Department establish formal policies and procedures to clear sensitive information and software from computers, disks, and other media prior to their disposal.

Management Response:
"Agree. The Department does clear sensitive information and software from computers and disks and other media before disposal. This process will be documented."

Approximate Date of Expected Completion:
June 30, 2004.

EX.15: Microsoft SQL Server

Finding:
The Department has not taken the necessary measures to reduce the risk of unauthorized access to the database server supporting the eSchoolPlus application. Our evaluation of the Windows® 2000 server running SQL Server identified a system configuration that was vulnerable to unauthorized access. SQL Server security is tightly coupled to the operating system and, by default, Microsoft® Windows® 2000 installations contain numerous potential security problems including several unneeded services that are installed and enabled, minimal event logging, and no active local security policy. The Department did not make the appropriate modifications to the operating system's default configuration to adequately safeguard the database server from potential vulnerabilities.

Recommendation:
We recommend the Department develop and implement a standard system configuration based upon manufacturer's security hardening recommendations or "best practices" to significantly reduce the risk of unauthorized access to be used for all Microsoft® Windows® 2000 computers running SQL Server.

Management Response:
"Agree. The Department for its DDOE environment does meet these standards. TMD will implement the same system for its eSchoolPlus product."

Approximate Date of Expected Completion:
August 15, 2004.

EX.16: Logical Security

Finding:
The Department is not enforcing a strong password policy for user accounts accessing the eSchoolPlus application. With the increase in computer processing power and the free availability of password cracking tools it is crucial that a strong password policy be implemented for all accounts. Poor password parameters subject sensitive information to potential unauthorized access and prevent Department system administrators from detecting unauthorized access on their systems.

The Department of Technology and Information's *Acceptable Use Policy* suggests the following password policy:

- Be at least seven characters
- Consist of a mix of at least three of the following: English uppercase, English lowercase, numeric, special characters
- Not contain your user name or name
- Not be a common word or name

Recommendation:
We recommend the Department implement a strong password policy for the user accounts accessing the eSchoolPlus application. Due to the sensitivity of the data contained in the eSchoolPlus application, the password policy should include, but not be limited to be at least 8 characters long, not greater than a 45 day limit, should lock-out a user for a determined period of time after 5 unsuccessful logon attempts, and should not be re-used on the same or other systems.

We further recommend that the Department require all users to immediately change their password to comply with the strong password policy.

Management Response:
"Agree. The Department for its DDOE environment does meet these standards. TMD will implement the same system for its eSchoolPlus product."

Approximate Date of Expected Completion:
August 15, 2004.

EX.17: Software Inventory

Finding:
Accurate and complete software inventory records are not being maintained. The Department has not developed formal policies and procedures to identify and ensure accountability of software. A Software inventory should include a description of the software, manufacturer, serial number or other identification number, the funding source, location, acquisition date, cost and date of disposal. Adequate software documentation would not only ensure accountability but would also ensure that the software is licensed and up to date. Unlicensed software constitutes copyright infringement, for which the Department may be subject to civil and/or criminal penalties and outdated software may contain defects, incomplete files, or inadequate documentation.

Recommendation:
We recommend the Department perform a thorough inventory of all software maintained\owned by the Department.

We further recommend the Department establish formal policies and procedures for maintaining complete and accurate inventory records of software to include periodic (i.e. annual) verifications and reconciliations of software be performed.

Management Response:
"Agree. The Department will initiate this finding and TMD will conduct an inventory."

Approximate Date of Expected Completion:
Policies: June 30, 2004.
Inventory: June 30, 2005.

EX.18: Training Documentation

Finding:
Management does not document or monitor employee training and professional development accomplishments for IT personnel. Management should monitor employee training and professional development accomplishments to ensure that employees, including data owners, system users, data processing personnel, and security management personnel, have the expertise to carry out their information security responsibilities. Failure to monitor employee training and professional development could result in a lack of expertise required to carry out responsibilities with regard to the eSchoolPlus application and other departmental systems.

Recommendation:
We recommend that management document and monitor employee training and professional development accomplishments for IT personnel.

Management Response:
"Agree. Appropriate policies and procedures will be developed."

Approximate Date of Expected Completion:
December 31, 2004.

EX.19: Uninterruptible Power Supply (UPS) Physical Security

Finding:
The location of the UPS used to supply immediate backup power for all Department equipment located in the computer room does not provide for adequate physical security. Access to the UPS, located outside the computer room, is easily accessible via an adjoining agency's office space. Access should be limited to personnel with a legitimate need for access to perform their duties. By obtaining unrestricted access to the UPS, an individual could cause intentional or unintentional loss or impairment.

Recommendation:
We recommend the Department ensure the UPS is located in a physically secured area.

Management Response:
"Agree. In progress. Working with Administrative Services."

Approximate Date of Expected Completion:
Unknown.

EX.20: Database Access

Finding:
A user working for a school district has been granted direct access to databases stored on the database server supporting the eSchoolPlus application. This user was identified by the Department as an end-user requiring access to the databases for downloading "real-time" data from a reporting database that is to be used in several ad-hoc reports generated by the school district. At the time of our review, the user had been given read, write, insert, and update access to two production databases stored on the database server. A proper segregation of duties should prohibit developers from having access to production data. By granting insert, write, and update access this user may directly connect to the production database server and modify or add data to the databases for which he has been granted access thereby circumventing the controls of the eSchoolPlus application. In addition to circumventing the eSchoolPlus application controls, allowing users to connect directly to the database server substantially increases the risk of data

tampering, unauthorized disclosure of information, loss of control over system integrity, and interruptions in providing computer services.

Recommendation:
We recommend the Department modify this user's database access to be read-only to the appropriate databases.

Management Response:
"Agree. In progress. "

Approximate Date of Expected Completion:
Development environment will be completed by August 31, 2004.

EX.21: Incident Response

Finding:
We found the Department does not have documented policies and procedures for detecting, reporting, and responding to computer security incidents. Without prompt and appropriate responses to security incidents, violations could continue to occur and cause damage to an entity's resources indefinitely. In addition, violators will not be deterred from continuing inappropriate access activity, which could result in losses and disclosure of confidential information. To be effective, information security responsibilities should clearly delineate responsibilities and expected behavior of all individuals with access and should be clear about the consequences of behavior not consistent with the rules.

Recommendation:
We recommend the Department establish formal policies and procedures for responding to security violations. Policies should include procedures and criteria for:

- documenting offenses,
- determining the seriousness of violations,
- reporting violations to higher levels of management,
- investigating violations
- imposing disciplinary action for specific types of violations,
- notifying the resource owner of the violation, and
- reporting suspected criminal activity to law enforcement officials.

Management Response:
"Agree. Policies and procedures will be developed as recommended."

Approximate Date of Expected Completion:
June 30, 2004.

DISTRIBUTION OF REPORT

Copies of this report have been distributed to the following public officials:

Legislative

The Honorable Russell T. Larson, Controller General, Office of the Controller General

Executive

The Honorable Ruth Ann Minner, Governor, State of Delaware
The Honorable Jennifer W. Davis, Budget Director, Office of the Budget

Other Elective Offices

The Honorable M. Jane Brady, Attorney General, Office of the Attorney General

Other

The Honorable Valerie A. Woodruff, Secretary of Education, Department of Education
Ms. Robin R. Taylor, Associate Secretary, Department of Education
Ms. Becki Surguy, CPA, FMS Specialist, Division of Accounting